

Notice of Allowability

Application No.

09/770,525

Applicant(s)

HRABIK ET.AL.

Examiner

Art Unit

Jenise E. Jackson

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/17/06.
2. ☒ The allowed claim(s) is/are 23,25-30,32,33,35 and 37-42.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 20060907
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

CHRISTOPHER REVAK
PRIMARY EXAMINER

cel 9/16/06

Examiner's Amendment

The Examiner contacted Anna Vishev, Attorney of record, on September 5, 2006. Ms. Vishev agreed to the following amendments that are highlighted in bold letters and underlined.

Please **enter these changes** that are in bold letters and underlined.

The application has been amended as follows:

Claim 23. A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:

(a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network and detect attacks on the at least some devices;

(b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and

(c) a first secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first secure link, **wherein the master system further monitors whether the security subsystem responds to the master system, the master system taking action if no response is detected.**

Claim 33. A security system for a computer network, the network having a plurality of devices connected thereto, at least some of the devices having security-related functions, the security system comprising:

(a) a security subsystem associated with at least some of the devices in the network which tests the integrity of the security-related functions;

Art Unit: 2131

(b) a master system which monitors the integrity of the security subsystem and receives and stores results of the integrity testing of the devices having security-related functions; and

(c) a secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the results of the integrity testing of the devices having security-related functions through the first secure link,

wherein one of the master system and the security subsystem further monitors whether a device having security-related functions responds to said one of the master system and the security subsystem, and wherein one of the security subsystem and the master system takes action when no response is detected.

Claim 42. A security system for a computer network, the network having a plurality of devices connected thereto, the security system comprising:

(a) a security subsystem connected to at least some of the devices in the network, the security subsystem configured to monitor activities of the at least some devices on the network, and detect attacks on the at least some devices;

(b) a master system which monitors the integrity of the security subsystem and registers information pertaining to attacks detected by the security subsystem; and

(c) a first secure link connected between the security subsystem and the master system, the master system monitoring the integrity of the security subsystem and receiving the information pertaining to the attacks through the first secure link, **wherein one of the master system and the security subsystem further monitors whether the device responds to one of the master system and the security subsystem, and wherein one of the security subsystem and the master system takes action when no response is detected.**

Reasons For Allowance

1. ***Status of Claims:*** Claims 31, 36-38 were objected to in the previous office action dated, 12/19/05. The Applicant has amended independent claims 23, 33, and 42 to include the limitation of claim 31 which was an objected to claim in previous office action 12/19/05. Claims 23, 25-30, 32-33, 35, 37-42 are allowable for the reasons listed below:

2. The claimed invention states that a major shortcoming of security systems is that they reside on the same network. Thus, when an intruder has gained access to the network, the whole network is attacked and is vulnerable. The same network on which a security system resides is also vulnerable. Non-patent literature Emigh, teaches a company that has 24/7 monitoring, intervention, testing, and trend analysis from IBM's Network Security Operations Center in Colorado. Netranger sensors are located at places on a corporate network such as the Internet and intranet connections, together with the intrusion monitor to be used by IBM at the NSOC. The sensor will look into the data stream, analyzing it for signatures indicative of misuse. If misuse is found, an alarm will be sent in real-time to Colorado. The claim limitation of "wherein the master system further monitors whether the security subsystem responds to the master system, the master system taking action if no response is detected", is not taught in Emigh. The master system of Emigh is the NSOC, the NSOC provides 24/7 monitoring, and the security subsystem is the network sensor located on the network, if a misuse if found an alarm is sent. There is no suggestion or teaching of if the security subsystem does not response the master

Art Unit: 2131

system taking action. Further, Emigh teaches that IBM's NSOC gives written reports to customers of the status of the network, thus there is no teaching of master system taking action.

3. The non-patent literature of Messmer teaches, a company called Counterpane Internet Security that has a managed intrusion detection service. Counterpane's service monitors the customer's internal servers and network traffic. A probe is put on the customer's network to accept audit data from a wide range of devices. The counterpane's black box sensor captures syslog and audit outputs from servers, firewalls, and intrusion detection software. The counterpane box regularly transmits the network activity output in encrypted from the Counterpane's data centers. Counterpane advises corporations on how to combat threats but do not make changes to the corporation's equipment. The claim limitation of "wherein the master system further monitors whether the security subsystem responds to the master system, the master system taking action if no response is detected", is not taught in Messmer. The black box regularly transmits information to the master system(i.e. data center). There is no suggestion or disclosure of "wherein the master system further monitors whether the security subsystem responds to the master system, the master system taking action if no response is detected". Further, Messmer teaches that the Master system does not take action as claimed by the Applicant, because Messmer teaches that Counterpane advises corporations on how to combat threats but do not make changes to the corporation's equipment.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2131

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791.

The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

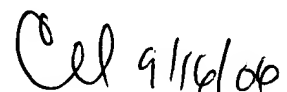
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



September 7, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER



9/16/06